VICTOR JIH, State Bar No. 186515
Email: vjih@wsgr.com
SOPHIA M. MANCALL-BITEL, State Bar No. 337002
Email: smancallbitel@wsgr.com
WILSON SONSINI GOODRICH & ROSATI
Professional Corporation
1900 Avenue of The Stars, 28th Floor
Los Angeles, CA 90067
Telephone: (424) 446-6900
Facsimile: (866) 974-7329

ANTHONY J WEIBELL, State Bar No. 238850
Email: aweibell@wsgr.com
WILSON SONSINI GOODRICH & ROSATI
Professional Corporation
650 Page Mill Road
Palo Alto, California 94304-1050
Telephone: (650) 493-9300
Facsimile: (866) 974-7329

Attorneys for Defendants
TikTok Inc. and ByteDance Inc.

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA, WESTERN DIVISION

BERNADINE GRIFFITH; PATRICIA SHIH; RHONDA IRVIN; MATHEW RAUCH; JACOB WATTERS, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

TIKTOK, INC., et al.,

Defendants.

Case No.: 5:23-cv-00964-SB-E

DEFENDANTS TIKTOK INC. AND BYTEDANCE INC.'S REPLY IN SUPPORT OF MOTION TO DISMISS PLAINTIFFS' FIRST AMENDED COMPLAINT UNDER FED. R. CIV. P. 12(b)(6)

Judge: Hon. Stanley Blumenfeld, Jr.
Date: December 15, 2023
Time: 8:30 a.m.
Place: Courtroom 6C

Action Filed: May 26, 2023
Trial Date: September 30, 2024

TABLE OF CONTENTS

Page

I. INTRODUCTION 1

II. THE PRIVACY CLAIMS FAIL AS A MATTER OF LAW 2

A. "Surreptitious" Collection Does Not, On Its Own, Violate Privacy Rights–and TikTok Did Nothing Surreptitious 2

B. Because the Pixel is Page-Based Tech, Plaintiffs Cannot Plausibly Allege Privacy Violations Without Page-Specific Allegations 3

C. Plaintiffs (Non-TikTok Users) Have Not Stated a Privacy Claim Because They Do Not Allege the Collection of Identifiable Data 6

III. THE INTERCEPTION CLAIMS FAIL AS A MATTER OF LAW 7

A. Plaintiffs Do Not Identify Any "Contents" of Any Communications Collected From Them 7

B. Plaintiffs' New Allegations Make Clear That TikTok Did Not Cause any Unlawful Interception or Recording 8

IV. THE PROPERTY CLAIMS FAIL AS A MATTER OF LAW 10

V. THE CFAA CLAIM FAILS AS A MATTER OF LAW 11

VI. THE UCL CLAIM FAILS AS A MATTER OF LAW 13

VII. UNJUST ENRICHMENT FAILS AS A MATTER OF LAW 14

VIII. CONCLUSION 15

TABLE OF AUTHORITIES

Page(s)

CASES

Ashcroft v. Iqbal,
556 U.S. 662 (2009) 3, 11, 15

Astiana v. Hain Celestial Grp., Inc.,
783 F.3d 753 (9th Cir. 2015) 14

Bell Atlantic Corp. v. Twombly,
550 U.S. 544 (2007) 6, 15

Bowyer v. Hi-Lad, Inc.,
216 W. Va. 634 (2004) 9

Brown v. Google LLC,
2023 WL 5029899 (N.D. Cal. Aug. 7, 2023) 7, 14

Calhoun v. Google LLC,
526 F. Supp. 3d 605 (N.D. Cal. 2021) 10, 11

Calhoun v. Google LLC,
No. 4:20-cv-05146-YGR (N.D. Cal. Nov. 9, 2020), ECF No. 67 10

Cappello v. Walmart Inc.,
2019 WL 11687705 (N.D. Cal. Apr. 5, 2019) 4

Castel S.A. v. Wilson,
2020 WL 4003024 (C.D. Cal. July 15, 2020) 14

Colo. Republican Comm. v. Doe,
2016 WL 3922156 (D. Colo. July 21, 2016) 13

Cook v. GameStop, Inc.,
2023 WL 5529772 (W.D.Pa. Aug. 28, 2023),
appeal filed, No. 23-2574 (3d Cir. Aug. 29, 2023) 5, 8

Cousin v. Sharp Healthcare,
2023 WL 4484441 (S.D. Cal. July 12, 2023) 4, 9

CTC Real Estate Servs. v. Lepe,
40 Cal. App. 4th 856 (2006) 10

Del Vecchio v. Amazon.com, Inc.,
2012 WL 1997697 (W.D. Wash. June 1, 2012) 11

Farst v. Autozone, Inc.,
2023 WL 7179807 (M.D. Pa. Nov. 1, 2023) 5

Fed. Deposit Ins. Corp. v. Dintino,
167 Cal. App. 4th 333 (2008) (2008) 15

Fraley v. Facebook, Inc.,
830 F. Supp. 2d 785 (N.D. Cal. 2011) 10, 11

Gershzon v. Meta Platforms, Inc.,
2023 2023 WL 5420234 (N.D. Cal. Aug. 22, 2023) 7

Hamm v. Wyndham Resort Dev. Corp.,
2020 WL 1853577 (M.D. Tenn. Apr. 13, 2020) 3

Hammerling v. Google LLC,
615 F. Supp. 3d 1069 (N.D. Cal. 2022) 7

In re Anthem Inc. Data Breach Litig.,
2016 WL 3029783 (N.D. Cal. May 27, 2016) 11

In re Facebook, Inc. Consumer Privacy User Profile Litig.,
402 F. Supp. 3d 767 (N.D. Cal. 2019) 15

In re Facebook Inc. Internet Tracking Litig.,
956 F.3d 589 (9th Cir. 2020) ..... *passim*

In re Facebook Priv. Litig.,
572 F. App'x 494 (9th Cir. 2014) 11

In re Google Inc. Cookie Placement Consumer Priv. Litig.,
806 F.3d 125 (3rd Cir. 2015) 7

In re Google RTB Consumer Priv. Litig.,
606 F. Supp. 3d 935 (N.D. Cal. 2022) 7

In re Marriott Int'l, Inc. Customer Data Sec. Breach Litig.,
440 F. Supp. 3d 447 (D. Md. 2020) 11

In re Meta Pixel Healthcare Litig.,
647 F. Supp. 3d 778 (N.D. Cal. 2022) 7

In re Yahoo! Inc. Customer Data Sec. Breach Litig.,
2017 WL 3727318 (N.D. Cal. Aug. 30, 2017) 11

Ind. v. TikTok, Inc.,
No. 02D03-2212-PL-401 (Ind. Super. Ct. Nov. 29, 2023) 2

Johnson v. Auto. Club of S. Cal.,
2013 WL 5832236 (Cal. Ct. App. Oct. 30, 2013) 3

Knuttel v. Omaze, Inc.,
2022 WL 1843138 (C.D. Cal. Feb. 22, 2022) 14

Korea Supply Co. v. Lockheed Martin Corp.,
29 Cal. 4th 1134 (2003) 15

Lopez v. Apple Inc.,
519 F. Supp. 3d 672 (N.D. Cal. 2021) 9

Popa v. PSP Grp., LLC,
2023 WL 7001456 (W.D. Wash. Oct. 24, 2023) 6

Promedev, LLC v. Wilson,
2023 WL 2330377 (W.D. Wash. Mar. 2, 2023) 3

Revitch v. New Moosejaw, LLC,
2019 WL 5485330 (N.D. Cal. Oct. 23, 2019) 9

Varkonyi v. United Launch All., LLC,
2023 WL 4291649 (C.D. Cal. May 12, 2023) (Blumenfeld, J.) 13

Williams v. DDR Media, LLC,
2023 WL 5352896 (N.D. Cal. Aug. 18, 2023) 2

STATUTES

18 U.S.C. § 2511 10

18 U.S.C. § 2511(a) 9

18 U.S.C. § 2512 10

Cal. Civ. Code § 1798.120(a) 11

Cal. Civ. Code §1798.140(v)(1) 11

Cal. Penal Code § 631 10

Cal. Penal Code § 631(a) 8

Cal. Penal Code § 632(a) 9

Cal. Penal Code § 635 10

MISCELLANEOUS

Surreptitious, Black's Law Dictionary (11th ed. 2019) 3

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

Plaintiffs act as if the Court has already ruled on the issues raised by Defendants' Motion and urge it to simply adopt the same result. But the First Amended Complaint ("FAC") adds new allegations, new plaintiffs, and new claims. Unless the new does not matter, their inclusion requires analysis. In fact, these new allegations confirm that the claims have no merit.

The FAC provides greater detail about how the Pixel works and the respective roles of TikTok and the websites who install it. As the new allegations explain, TikTok programs the Pixel to share routine information—such as IP address, browser agent, and URL—the same basic information always shared to networked computers and ISPs because that is how the Internet works. Absent special circumstances, this basic sharing does not state a claim. For the Pixel to share anything else, it must be configured by the websites who install the Pixel.

The FAC also acknowledges that the Pixel is page-based technology. What the Pixel discloses depends on what webpage it is on. This is similar to a homeowner with a security camera. The security camera is a tool that its owner can use to record what they want. There are no issues if the camera is placed outside a homeowner's front door. But there are serious problems if they place the same camera in a public restroom. The same can be said about the Pixel—whether any privacy rights are violated depends on the page it is placed on, the sensitivity of what appears or is entered on that page, and the configuration of that page and the Pixel. In short, any claim for using the Pixel depends on the circumstances of its use. Those circumstances are determined by the websites, not TikTok.

These new details require a reanalysis of Plaintiffs' claims. Coupled with new problems Defendants have identified, they cast the claims in an entirely new light. It is now clear this case is materially different from *Facebook Tracking*. It is

also clear TikTok does not directly cause any intrusion, interception, or recording. Claiming property rights over such routine online information remains suspect. And the same problems with the CFAA and UCL claims persist. Taken together, the FAC confirms these claims have no merit and should be dismissed.

II. THE PRIVACY CLAIMS FAIL AS A MATTER OF LAW

Plaintiffs continue to base their privacy claims on *Facebook Tracking*'s "primary holding" that "an allegation of surreptitious mass collection of referrer and full-string URLs is sufficient." Opp. at 7, ECF No. 75. This is wrong and that case does not dictate the outcome of this case. First, *Facebook Tracking* never held that "surreptitious" collection is enough, and TikTok was not surreptitious. Second, that case concerned different technology. Third, those claims were brought by Facebook users (known to Facebook) and not by non-users.

A. "Surreptitious" Collection Does Not, On Its Own, Violate Privacy Rights–and TikTok Did Nothing Surreptitious

"Surreptitious" collection, without other problematic conduct, does not state a privacy claim. *Williams v. DDR Media, LLC*, 2023 WL 5352896, at *5-7 (N.D. Cal. Aug. 18, 2023) (even though these users were not informed of the collection, no privacy violation). The secret collection of data, even a lot of data, does not mean that an individual's privacy rights were violated; it also depends on the nature of the data collected. *Facebook Tracking* does not stand for the proposition that surreptitious conduct is sufficient for a claim.

And TikTok's collection was not "surreptitious." The Pixel is not a secret; TikTok explains in detail on its public website how the technology works. *Ind. v. TikTok, Inc.*, No. 02D03-2212-PL-401, at *22 (Ind. Super. Ct. Nov. 29, 2023) (failure to provide specific disclosures was not "deceptive" as a matter of law). Plaintiffs' FAC even relies on those explanations as the basis for their claims. *See, e.g.*, FAC ¶ 49, ECF No. 63 (citing TikTok's webpage disclosing what information the Pixel collects without configuration and the use of first-party and third-party

cookies); *id.* ¶ 52 (citing TikTok's webpage about additional events websites can configure). The Pixel and TikTok's data collection was reported by the press, and the FAC incorporates many of those reports. *See, e.g.*, FAC ¶¶ 49, 61, 66.

When someone discloses what they are doing, that conduct is not surreptitious. *See Surreptitious*, Black's Law Dictionary (11th ed. 2019) ("surreptitious" means "unauthorized and clandestine; done by stealth and without legitimate authority"); *Promedev, LLC v. Wilson*, 2023 WL 2330377, at *5, 6-7 (W.D. Wash. Mar. 2, 2023) (no wrongdoing where the facts were publicly available). It does not matter that Plaintiffs allegedly did not know, read, or understand the TikTok Pixel. *See Johnson v. Auto. Club of S. Cal.*, 2013 WL 5832236, at *4 (Cal. Ct. App. Oct. 30, 2013) (plaintiff "was not deceived; rather, she failed to read"); *Hamm v. Wyndham Resort Dev. Corp.*, 2020 WL 1853577, at *11 (M.D. Tenn. Apr. 13, 2020) (one cannot be deceived by failing to read what was made available to them). Plaintiffs' conclusory allegation that the collection here was "surreptitious" should be disregarded. *See Ashcroft v. Iqbal*, 556 U.S. 662, 678-79 (2009).

This case bears no resemblance to *Facebook Tracking*. Facebook promised its users that it would not collect data when users are logged out, but then did precisely that. That case was riddled with internal evidence acknowledging this misrepresentation and the privacy problem created by its practice. *See In re Facebook Inc. Internet Tracking Litig.*, 956 F.3d 589, 596-97, 601-02 (9th Cir. 2020). In fact, Facebook stopped the practice after a blogger publicly identified it—suggesting it intended to keep this collection secret from users. *Id.* at 596-97.

B. Because the Pixel Is Page-Based Tech, Plaintiffs Cannot Plausibly Allege Privacy Violations Without Page-Specific Allegations

Plaintiffs admit that the Pixel is page-based technology—it must be installed on each webpage a website owner deems important, its configuration can differ page to page, and what it discloses depends on the page. *See* FAC ¶¶ 49 (Pixel

event must fire to transmit data; it fires when visitor views a particular page), 52 (websites configure Pixel to capture certain data on a page). This is consistent with how courts have understood pixel technology. *See, e.g.*, *Cousin v. Sharp Healthcare*, 2023 WL 4484441, at *3 (S.D. Cal. July 12, 2023) (plaintiff must identify if activities occurred on page with pixel); *Cappello v. Walmart Inc.*, 2019 WL 11687705, at *1 (N.D. Cal. Apr. 5, 2019) (pixel loads on a particular page).

Because the Pixel is page-based, Plaintiffs must make page-specific allegations. *See Cousin*, 2023 WL 4484441, at *3 (dismissing claim for failure to allege page-specific activities). It is not enough to say that Pixel is used on "Riteaid.com." *See id.*; FAC ¶ 110. Plaintiffs must allege that it is used on a webpage they visited, that they entered sensitive and identifying information on that page, and that the configuration of the Pixel and that page resulted in the disclosure of that private information. Without such allegations, there is no plausible claim. Like the security camera, a privacy violation depends on location.

This reveals a glaring problem—Plaintiffs assiduously avoid page-specific allegations. The FAC relies on generalities and speaks only in terms of a website's decision to install the Pixel. Plaintiffs cannot mask these deficiencies by repeating the mantra that this case is just like *Facebook Tracking*. It is not.

First, the page-specific Pixel technology works differently than a plug-in. *Facebook Tracking* analyzed a browser extension that changes the program being used. *See* 956 F.3d at 596 n.1. The plug-in did not merely disclose information about the specific page on which the plug-in is embedded, but also information about every other page on any website a visitor may visit that has any Facebook plug-in embedded. *Id.* at 605 (Facebook plug-in collected Google links with search terms input on that site). The *Facebook Tracking* court noted that simply disclosing what page someone visited is not the privacy problem. *Id.* at 604-05. Those aspects of the plug-in technology are not present here. This case is based on

search terms a user may input on the specific page that has the Pixel installed. *See, e.g.*, Opp. at 7, 13-14. These different technologies pose different privacy risks.

Second, Plaintiffs fail to articulate what information they entered on a Pixel-embedded page, if any. They only allege that the Pixel "was installed on" public websites such as Rite-Aid and The Vitamin Shoppe. FAC ¶¶ 110, 128, 134, 135, 136. Rite-Aid is a pharmacy, but it also sells candy and school supplies. The Vitamin Shoppe sells health supplements and foods. Plaintiffs do not allege that the Pixel was on a page for a specific, sensitive medication or supplement. Browsing the aisle of one of these storefronts is not sensitive, nor is visiting the web store. *Farst v. Autozone, Inc.*, 2023 WL 7179807, at *4 (M.D. Pa. Nov. 1, 2023). Plaintiffs do not identify a single search or action on any page, let alone anything sensitive. They do not allege, for instance, that they entered sensitive information "such as searches for medical conditions, contraceptives, and addiction treatment facilities." Order at 8 n.4, ECF No. 59.

Third, Plaintiffs do not allege what information the URLs of pages they visited revealed. They offer generalized allegations about what certain URLs "could" show (e.g., on webpages for charitable donations, food delivery or flight booking). FAC ¶ 51. It is not enough for Plaintiffs to allege the data could reveal their information. *Cook v. GameStop, Inc.*, 2023 WL 5529772, at *7 (W.D.Pa. Aug. 28, 2023), *appeal filed*, No. 23-2574 (3d Cir. Aug. 29, 2023). Plaintiffs must offer facts showing that their information was disclosed via the URLs of the pages they visited. Because the Pixel is embedded on specific webpages, this is easy to determine. *See* FAC ¶ 52 n.45 (citing TikTok Business Help Center).

The Court cannot assess the plausibility of the privacy claims without page-specific allegations. Plaintiffs should be required to answer these basic questions: Did they visit a webpage where the Pixel was embedded? Did they enter search terms or anything sensitive? Did that page have a full-string URL that revealed

those terms or anything sensitive? There is no reason to give Plaintiffs a pass—they know the answers. They should not be allowed to obscure these problems with generalities. The entire purpose of this motion is to suss out unviable claims. *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007).

C. Plaintiffs (Non-TikTok Users) Have Not Stated a Privacy Claim Because They Do Not Allege the Collection of Identifiable Data

Plaintiffs concede that they cannot state a claim based on the collection of anonymized or non-identifiable information. *Popa v. PSP Grp., LLC*, 2023 WL 7001456, at *5 (W.D. Wash. Oct. 24, 2023) (distinguishing *Facebook Tracking* because no allegation plaintiff entered identifying information). Conclusory allegations that do not mention any Plaintiff are insufficient. *See* Order at 8 n.4.

Instead, Plaintiffs cling to the conclusion that their allegations "are materially indistinguishable from those in *Facebook Tracking*." Opp. at 11. But the data collected in *Facebook Tracking* was per se identifiable because the plaintiffs were Facebook users. 956 F.3d at 599. Facebook placed cookies on the computers of its own users. *Id.* at 596. Facebook could thus directly connect that browsing data with users' personal profiles, through which they provided their identity information and other personal data—that was the privacy problem. *Id.*

This case is very different. Plaintiffs are non-TikTok users. FAC ¶ 1. They did not provide to TikTok the types of identifying information that Facebook's users provide. That is why TikTok must undertake the process of trying to match data with a known TikTok user. September 8, 2023, Hearing Tr. at 30:3-21. The Opposition strings together a handful of conclusory allegations, *see* Opp. at 11, but none allege that identifying information was taken. Four of the Plaintiffs claim they could not have registered for an account or made a purchase on Rite-Aid or The Vitamin Shoppe had they not entered identifying information. *Id.* But none of this appears in the FAC. Plaintiffs still avoid specifying whether they provided their own email or physical addresses, credit card numbers or even their real

names. Nor do they allege that the Pixel ran on any page where they registered or made a purchase, or that it was configured to disclose identifying information.

III. THE INTERCEPTION CLAIMS FAIL AS A MATTER OF LAW

A. Plaintiffs Do Not Identify Any "Contents" of Any Communications Collected From Them

The same problems plague the CIPA and ECPA claims. Both sides agree that only the collection of "contents" can state a CIPA or ECPA claim. Opp. at 13. The standard for "contents" under CIPA and ECPA are the same. *Id.* The parties also agree that URLs can constitute contents. *Id.* Determining "contents" is "a contextual 'case-specific' analysis." *Hammerling v. Google LLC*, 615 F. Supp. 3d 1069, 1092 (N.D. Cal. 2022) (citation omitted). It "hing[es] on how much information would be revealed by the information's tracking and disclosure." *Id.*

To meet this standard, Plaintiffs must allege how the URL of the pages they visited disclosed the contents of their communications with specific examples. The cases Plaintiffs cite highlight the deficiency of the FAC. Those cases were allowed to proceed because these specifics were present.[1] *See Gershzon v. Meta Platforms, Inc.*, 2023 WL 5420234, at *3 (N.D. Cal. Aug. 22, 2023) (https://www.dmv.ca.gov/portal/?s=how+do+I+renew+disabled+parking +placard); *In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d 778, 795-96 (N.D. Cal. 2022) (hardfordhospital.org/services/digestive-health/conditions-we-treat/colorectal-small-bowel-disorders/ulcerative-colitis); *Brown v. Google LLC*, 2023 WL 5029899, at *15 (N.D. Cal. Aug. 7, 2023) (https%3A%2F%2Fwww. washingtonpost.com%2Fworld %2F2022%2F2%2F18%2Frussia-ukraineupdates%2F).

[1] *Google RTB* and *Google Cookie Placement* do not contradict this requirement. The first alleged the collection of more than URLs. *In re Google RTB Consumer Priv. Litig.*, 606 F. Supp. 3d 935, 949 (N.D. Cal. 2022). In the second, Google conceded that some of the collected URLs were "contents." *In re Google Inc. Cookie Placement Consumer Priv. Litig.*, 806 F.3d 125, 139 (3rd Cir. 2015).

The FAC alleges none of these critical details. Plaintiffs do not discuss the contents of the URLs they allege were taken. Nor do they mention whether new URLs were generated from their "searching and browsing" and whether any resulting URL actually revealed the things they searched for. *See Cook*, 2023 WL 5529772, at *7. They do not even offer an example URL for a page they visited.

This is not a tall order. Plaintiffs know what websites they visited and search terms they entered. After all, they plead which websites they visited and that they generally "searched and browsed" on those websites. There is no reason why Plaintiffs would be unable to see the URLs that appear on the pages they visit. This information is under Plaintiffs' control. All they need to do is allege it.

The failure to specifically and plausibly allege "contents" requires the dismissal of these claims. This case is similar to *Cook*. Plaintiffs' allegations that they "searched and browsed" for goods, shows, jobs, and volunteer opportunities on the various websites are no more specific than the allegations rejected in *Cook*. *Cook*, 2023 WL 5529772, at *4 (plaintiff "communicated with GameStop's website by . . . typing search words into the search bar"). Likewise, Plaintiffs' allegations that the Pixel could collect full-string URLs containing search queries align with those rejected in *Cook*. *See, e.g.*, *id.* at *7 ("researchers have found that a variety of highly sensitive information can be captured in event responses from website visitors"). Without more specific allegations, the Court has "no way of knowing" whether any URL collected is contents or not. *Id.* at *9.

B. Plaintiffs' New Allegations Make Clear That TikTok Did Not Cause Any Unlawful Interception or Recording

The Opposition glosses over TikTok's causation argument by characterizing it as "already rejected." The Court, however, did not reject the argument; it recognized that causation matters. *See* Order at 12. To violate CIPA or ECPA, a defendant must be the direct cause of the interception or recording. This requirement comes from the statutes themselves. *See* Cal. Penal Code § 631(a)

(holding directly liable those who "willfully . . . read[], or attempt[] to read, or to learn the contents . . . of [a] communication"); Cal. Penal Code § 632(a) ("us[ing] a[] [device] to eavesdrop"); 18 U.S.C. § 2511(a) ("intentionally intercepts [or] endeavors to intercept"). The Court permitted Ms. Griffith's CIPA claims to proceed because it was unable to determine causation on the pleadings. *See* Order at 12. The Court was unable to determine who programmed and placed the Pixel.

The FAC now provides the missing detail. Plaintiffs allege that the Pixel's default setting includes PageView, which transmits the URLs of the pages that it is installed on. FAC ¶¶ 47, 52. The Opposition focuses on URL collection as the basis for Plaintiffs' claim. Opp. at 15. But Plaintiffs acknowledge that the Pixel is a page-based technology. FAC ¶¶ 49, 52; *see Cousin*, 2023 WL 4484441, at *3. The data collected varies depending on the page. Moreover, Plaintiffs recognize that the Pixel must be installed by the website for any information to be collected. *See, e.g.*, FAC ¶¶ 49, 53. And beyond PageView (and other record data), websites must configure additional settings to collect more information. *Id.* ¶¶ 49, 52, 230.

In other words, Plaintiffs concede that TikTok is not the direct cause of any interception or recording. That turns on who placed and configured the tool. In *Lopez*, Apple did. *See Lopez v. Apple Inc.*, 519 F. Supp. 3d 672, 679, 690 (N.D. Cal. 2021). Here, the websites do: they choose where to place the Pixel, place it, and configure it. *See* FAC ¶¶ 42, 49, 52.[2] By clarifying who causes any interception or recording, Plaintiffs plead themselves out of a direct liability claim. *See Bowyer v. Hi-Lad, Inc.*, 216 W. Va. 634, 652 n.10 (2004) (no liability on manufacturer of tool used by another to intercept).

[2] *Revitch v. New Moosejaw, LLC* is distinguishable, as (unlike here) plaintiff did not allege the websites' role in configuring the tool and never addressed causation. 2019 WL 5485330, at *2 (N.D. Cal. Oct. 23, 2019).

Nor do they plead secondary liability. Despite the Court's suggestion that liability may lie for manufacturing, distributing, or inducing, *see* Order at 11-12, the FAC alleges no such claims. Plaintiffs do not provide the necessary allegations (*i.e.*, that the Pixel is primarily or exclusively used for interception or eavesdropping). *See* Cal. Penal Code § 635; 18 U.S.C. § 2512. Nor do Plaintiffs allege that TikTok procured, induced, aided and abetted, or conspired with another to intercept or record communications. Cal. Penal Code § 631; 18 U.S.C. § 2511.

IV. THE PROPERTY CLAIMS FAIL AS A MATTER OF LAW

The parties' only dispute is whether Plaintiffs' browsing data is property. Plaintiffs again focus on the "growing trend" of cases recognizing the "property value of personal information." Opp. at 19-20 (citing *Calhoun v. Google LLC*, 526 F. Supp. 3d 605, 635 (N.D. Cal. 2021)). This does not mean Plaintiffs win. *Calhoun* speaks not only of the trend of recognizing the "property value of personal information," but also the need for "a property interest in . . . personal information." *Calhoun*, 526 F. Supp. 3d at 635 (emphasis added). The FAC's problem is that it is long on value and short on property.

Plaintiffs do not contest that a right to exclude is essential to a property interest. *See* Opp. at 19 (citing FAC ¶ 89). *Calhoun* and the cases it cites confirm that exclusion is needed. *Calhoun* rested on a contract-based right to exclude Google, since Google had promised not to collect "do not sync" data. Pls.' Opp'n to Mot. to Dismiss, *Calhoun v. Google LLC*, No. 4:20-cv-05146-YGR at 5, 20 (N.D. Cal. Nov. 9, 2020), ECF No. 67. *Facebook Tracking* did not reach the substance of the larceny claim, but the same contractual right to exclude Facebook would exist: Facebook promised not to collect logged-out data. 956 F.3d at 596-97. In *CTC Real Estate Servs. v. Lepe*, plaintiff's identifying information was property under an identity theft statute that provided a basis for exclusivity. 40 Cal. App. 4th 856, 860 (2006). In *Fraley v. Facebook, Inc.*, plaintiffs sued to

enforce their right of publicity under a statute granting them exclusive rights over likenesses. 830 F. Supp. 2d 785, 803 (N.D. Cal. 2011).[3]

The only basis Plaintiffs provide for a right to exclude is the California Consumer Privacy Act ("CCPA"). Plaintiffs say the Court must accept as true their allegation that the CCPA grants a right to exclude. *See* Opp. at 19. But that is a legal assertion that is false. *See Iqbal*, 556 U.S. at 678. The CCPA only grants a right to exclude businesses that sell or share consumers' personal information. Cal. Civ. Code § 1798.120(a). TikTok does not sell or share Plaintiffs' data. And the CCPA only grants a right to exclude identifiable data. Cal. Civ. Code § 1798.140(v)(1). Plaintiffs do not allege that they provided any identifiable data. Without a right to exclude, Plaintiffs fail to state property claims.

V. THE CFAA CLAIM FAILS AS A MATTER OF LAW

The Opposition continues to disregard the requirement that Plaintiffs allege CFAA harm caused by the alleged access to their computers. *See* Order at 14 (recognizing the threat must be caused by the alleged placement of cookies on Plaintiffs' computers). Plaintiffs still fail to show that TikTok's placement of cookies on their computers (the only "access" they identify) led to a "threat to public health or safety" (their only theory of harm). *See* Opp. at 18. Without this key allegation, Plaintiffs' claim must be dismissed. *See Del Vecchio v. Amazon.com, Inc.*, 2012 WL 1997697, at *5 (W.D. Wash. June 1, 2012).

Four of the five Plaintiffs (Ms. Griffith, Ms. Irvin, Mr. Rauch, and Mr. Watters) make no attempt to allege this causal link. *See* Order at 14. They

---

[3]The remaining cases cited by *Calhoun* are not about property. They discuss value in the context of damages or standing. *See In re Anthem Inc. Data Breach Litig.*, 2016 WL 3029783, at *14 (N.D. Cal. May 27, 2016) (damages); *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, 2017 WL 3727318, at *11-13 (N.D. Cal. Aug. 30, 2017) (standing); *In re Marriott Int'l, Inc. Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 461 (D. Md. 2020) (damages); *In re Facebook Priv. Litig.*, 572 F. App'x 494, 494 (9th Cir. 2014) (damages).

continue to rely entirely on the potential national security threat posed by TikTok's access to data generally. *See, e.g.*, FAC ¶ 176; Opp. at 17-18. This Court already recognized that this is not enough. *See* Order at 14. This Court's Order still applies to these claims with full force, so they must be dismissed. *See id.*

This leaves Ms. Shih. Her claim is predicated on allegations that she is a remote consultant for the Florida Department of Transportation; has "some" access to that agency's network, which, when she is connected to it, could provide access to internal data belonging to the agency; and was required to obtain Criminal Justice Information Services Level 4 certification. FAC ¶ 118; *see also* Opp. at 17.

None of this establishes a threat to public health or safety caused by the placement of cookies on her computer. Plaintiffs never specify the threat that could result if TikTok obtains access to some unidentified transportation and traffic information. *See* Mot. at 19-20. They hint that the data must be important based on Ms. Shih's certification. But that certification only demonstrates that Ms. Shih was trained in data security issues. *See* Fla. Dep't of Law Enforcement, *CJIS Online Systems for Non-Criminal Justice Agencies*, https://florida.cjisapps.com /noncrim/launchpad/cjisdocs/docs.cgi?cmd=FS&ID=51&TYPE=DOCS (May 2019). It says nothing about the type of data Ms. Shih may have access to—whether they are top secret documents concerning critical infrastructure or proposed bus fare increases or maintenance schedules.

Any threat is also entirely speculative. Through some fanciful Rube Goldberg chain of events, Plaintiffs claim that Etsy's use of the Pixel on its website poses a threat to public health and safety if Ms. Shih visits Etsy.com on her personal computer, because she also uses that computer to connect to the Florida Dept. of Transportation in her work as a remote consultant. The FAC never alleges that Ms. Shih visited Etsy while connected to any government network. The FAC never explains the scope of Ms. Shih's work as a remote consultant or

the types of specific files she has network access to. And the FAC never explains how the use of a Pixel on Etsy's website leads to the unauthorized access of any files on Ms. Shih's computer, let alone any files on other computers.

To state a CFAA violation, the threat to public health and safety must be real, not arbitrarily concocted. *See Colo. Republican Comm. v. Doe*, 2016 WL 3922156, at *2 (D. Colo. July 21, 2016). Speculation falls far short of this Court's standard requiring Plaintiffs to allege a plausible causal link between the CFAA harm and access to their computers. *See Varkonyi v. United Launch All., LLC*, 2023 WL 4291649, at *2 (C.D. Cal. May 12, 2023) (Blumenfeld, J.); Order at 14.

VI. THE UCL CLAIM FAILS AS A MATTER OF LAW

Plaintiffs attempt to meet the "[loss] of money or property" requirement for UCL standing through focus groups. Plaintiffs aver, without any facts, that TikTok makes their browsing data "available." Opp. at 20. Not so. If Plaintiffs had any specifics to support that false assertion, they would be alleged in the FAC. Based on that fiction, Plaintiffs claim "the value of their private data and of their participation in focus groups and surveys has been diminished." FAC ¶¶ 115, 124, 144. Besides being untrue, this makes no sense.

This Court has explained that Plaintiffs must plausibly allege specific facts showing: (1) a market for the data that was collected; and (2) an impaired ability to participate in that market. *See* Order at 16-17. Plaintiffs fail to do either.

First, Plaintiffs fail to plausibly allege the existence of a market for the data that was collected. There is no allegation that anyone conducting focus groups buys the historical browsing data collected. Surveys and focus groups depend on live answers to questions about specific products under controlled circumstances. *See* Mot. at 21. While the FAC identifies other markets for data generally, they do not cover the data collected here. *See* FAC ¶¶ 79 (black market for banking log-ins), 82 (programs run by other companies to buy unspecified browsing data).

Second, it is implausible that the Pixel impeded Plaintiffs' ability to participate in focus groups. Since Plaintiffs are not TikTok users and there is no allegation TikTok identified them or disclosed their identity, there would be no way for any focus group to reject Plaintiffs because of any TikTok data collection. *See* Mot. at 20-21. In addition, browsing data cannot supplant live participation in focus groups, so there is no reason to believe Plaintiffs would be barred on those grounds. *See id.* at 21. Plaintiffs do not even allege that the focus groups or surveys covered the same subject matter as their browsing data. *See id.* It is implausible that a company asking about curling irons or stoves would reject Ms. Griffith because it had access to her browsing data on buildabear.com.

Plaintiffs' only legal argument is that their claim resembles *Brown v. Google*. Opp. at 21. But in *Brown*, there was a market for the data because Google, the defendant collecting the data, had a program to pay for the same data it was collecting. *See Brown*, 2023 WL 5029899, at *6 ("Google itself piloted a program to pay users $3.00 a month to collect their browsing data."). Google collected the data at issue rather than paying plaintiffs under that program. *Id.* at *2. There are no such allegations here. Without them, there is no UCL claim.

VII. UNJUST ENRICHMENT FAILS AS A MATTER OF LAW

As this Court has held, California does not recognize an independent claim for unjust enrichment. *See, e.g.*, *Knuttel v. Omaze, Inc.*, 2022 WL 1843138, at *13 (C.D. Cal. Feb. 22, 2022) (citing *Astiana v. Hain Celestial Grp., Inc.*, 783 F.3d 753, 762 (9th Cir. 2015)). The Court "may construe a claim for unjust enrichment as a quasi-contract claim." *Id.* (emphasis added). But it is not required to do Plaintiffs' work by doing so. *See Castel S.A. v. Wilson*, 2020 WL 4003024, at *14 (C.D. Cal. July 15, 2020) (declining to construe UE claim as quasi-contract).

Nor have Plaintiffs stated a quasi-contract claim for restitution. The FAC seeks only disgorgement of profits, without regard to the alleged diminution of

value of Plaintiffs' data. *See* FAC ¶¶ 236-41. Restitution "is designed to restore the aggrieved party to his or her former position by return of the thing or its equivalent in money." *Fed. Deposit Ins. Corp. v. Dintino*, 167 Cal. App. 4th 333, 346 (2008) (citation omitted). Disgorgement of profits that is not tied to restoring lost money or property is non-restitutionary. *See Korea Supply Co. v. Lockheed Martin Corp.*, 29 Cal. 4th 1134, 1148-49 (2003).

Plaintiffs try to rewrite the FAC to base their claim on diminution of their data's value. *See* Opp. at 21. But Plaintiffs must provide more than a hypothetical economic injury. *See In re Facebook, Inc. Consumer Privacy User Profile Litig.*, 402 F. Supp. 3d 767, 784 (N.D. Cal. 2019) (no Article III standing). Plaintiffs must show their ability to profit from the data was impaired. *See id*. The Court dismissed Ms. Griffith's UCL claim because she did not do so. Order at 17. The FAC contains no such allegations. Thus, even if the Court were inclined to recast the unjust enrichment claim as quasi-contract, the claim should be dismissed.

VIII. CONCLUSION

The Motion identifies many holes in Plaintiffs' claims that raise serious questions as to whether any privacy right has actually been violated. Plaintiffs try to obscure them by focusing on the general. They eschew page-specific allegations even though this case concerns a page-based technology. To avoid the unnecessary expenditure of time and resources, though, Plaintiffs should not be given a "free pass" on these holes. Filling them does not require discovery. They may be factual, but Plaintiffs must still plead the facts so the Court can determine if they are plausible and, if assumed true, whether they state valid claims. The precise purpose of *Twombly* and *Iqbal* is to pierce the facade of any Potemkin Village and make sure there is substance to the claims before proceeding. The Court should reject Plaintiffs' attempt to state claims based on generalizations and fear mongering. Without specifics, the claims must be dismissed.

Dated: December 1, 2023

WILSON SONSINI GOODRICH & ROSATI
Professional Corporation

By: /s/ Victor Jih
Victor Jih

Attorney for Defendants
TIKTOK INC. and BYTEDANCE INC.

CERTIFICATE OF COMPLIANCE

The undersigned, counsel of record for Defendants TikTok Inc. and ByteDance Inc., certifies that this brief contains 5,118 words and does not exceed 15 pages, which complies with the word limit of L.R. 11-6.1. and this Court's Standing Order dated May 21, 2023.

Dated: December 1, 2023

WILSON SONSINI GOODRICH & ROSATI
Professional Corporation

By: /s/ Victor Jih
Victor Jih

Attorney for Defendants
TIKTOK INC. and BYTEDANCE INC.